PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-093254
(43)Date of publication of application : 07.04.1995

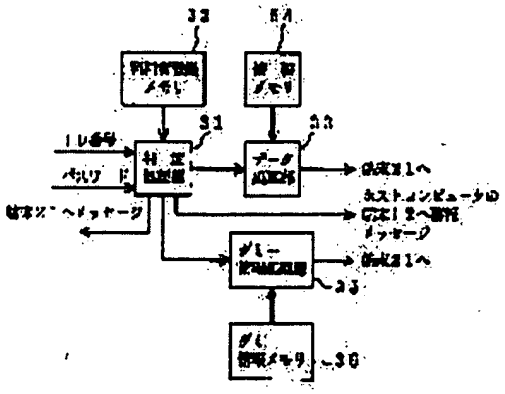
(51)Int.Cl. G06F 15/00
G06F 1/00
G06F 13/00

(21)Application number : 05-234412
(22)Date of filing : 21.09.1993

(71)Applicant : TOSHIBA CORP
(72)Inventor : MATSUMOTO KATSUNORI

(54) METHOD AND DEVICE FOR PREVENTING UNAUTHORIZED USE OF NETWORK SYSTEM

(57)Abstract:
PURPOSE: To prevent unauthorized use by preventing information from being outputted from a host computer to the third person by outputting an end message and disconnecting a terminal when wrong ID information is inputted by =n times.
CONSTITUTION: The host computer waits access from the terminal at all times, the terminal at the time of receiving access and becomes the state receiving an input from the terminal. In this state, when the ID number information is inputted from the terminal side to a judgement processing part 31, the judgement processing part 31 checks whether or not there are any relevant registered data in a user register memory 32, an when there are no registered data, an input error massage is issued to the terminal as abnormally. In this case, when the wrong ID number information sent from the terminal side is inputted at =n times, the end massage is issued to the terminal, and the terminal is disconnected. Further, when a wrong password is inputted by =n times, an alarm message is displayed at the terminal to inform a manager of abnormally.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平7－93254

(43)公開日　平成７年(1995)４月７日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ	15/00	３３０　Ｂ	7459－5Ｌ		
	1/00	３７０　Ｅ			
	13/00	３５１　Ｚ	7368－5Ｂ		

審査請求　未請求　請求項の数３　ＯＬ　（全　５　頁）

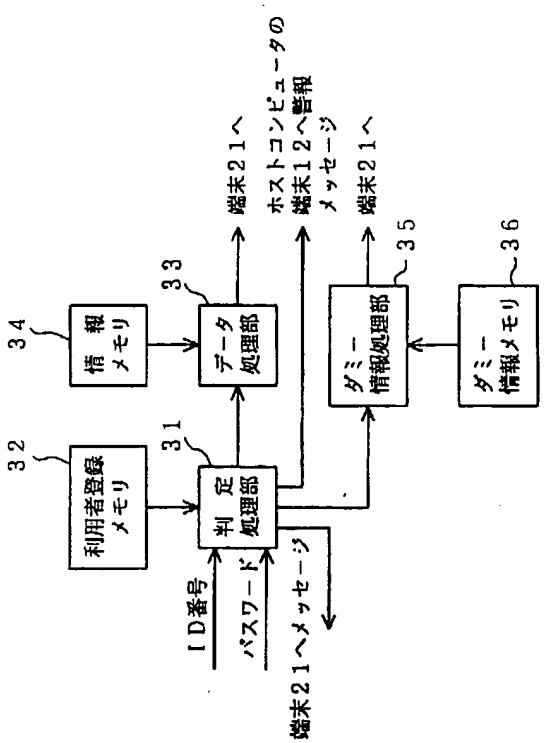
(21)出願番号　特願平5－234412

(22)出願日　平成５年(1993)９月21日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者　松本　克徳
東京都府中市東芝町１番地　株式会社東芝府中工場内
(74)代理人　弁理士　鈴江　武彦

(54)【発明の名称】　ネットワークシステムの悪用防止方法及び装置

(57)【要約】
【目的】ネットワークシステムにおける悪用を未然に防止すると共に、利用者の情報を保護することにある。
【構成】ホストコンピュータを中心に通信回線、ＬＡＮ等で接続された複数の端末を有し、且つ端末から送られるＩＤ番号情報及びパスワード情報が利用者登録と一致すると前記ホストコンピュータより端末に情報を出力可能にしたネットワークシステムにおいて、端末から送られるＩＤ番号情報及びパスワード情報を利用者登録データをもとにチェックし、ＩＤ番号情報が異常であるときは端末に入力エラーメッセージを出力し、さらに誤ったＩＤ情報がｎ回以上入力されると終了メッセージを出力して端末との接続を切離し、ＩＤ番号情報が正常でパスワード情報が異常のときは端末に入力エラーメッセージを出力し、さらに誤ったパスワード情報がｍ回以上入力されるとホストコンピュータの端末に警報メッセージを出力する。



1

【特許請求の範囲】

【請求項１】　ホストコンピュータを中心に通信回線、ＬＡＮ等で接続された複数の端末を有し、且つ端末から送られるＩＤ番号情報及びパスワード情報が利用者登録と一致すると前記ホストコンピュータより端末に情報を出力可能にしたネットワークシステムにおいて、前記端末から送られるＩＤ番号情報及びパスワード情報を利用者登録データをもとにチェックし、ＩＤ番号情報が異常であるときは端末に入力エラーメッセージを出力し、さらに誤ったＩＤ情報がｎ回以上入力されると終了メッセージを出力して端末との接続を切離し、ＩＤ番号情報が正常でパスワード情報が異常のときは前記端末に入力エラーメッセージを出力し、さらに誤ったパスワード情報がｍ回以上入力されると前記ホストコンピュータの端末に警報メッセージを出力することを特徴とするネットワークシステムの悪用防止方法。

【請求項２】　ホストコンピュータを中心に通信回線、ＬＡＮ等で接続された複数の端末を有し、且つ端末から送られるＩＤ番号情報及びパスワード情報が利用者登録と一致すると前記ホストコンピュータより端末に情報を出力可能にしたネットワークシステムにおいて、前記端末から送られるＩＤ番号情報及びパスワード情報を利用者登録データをもとにチェックし、ＩＤ番号情報が異常であるときは前記端末に入力エラーメッセージを出力し、さらに誤ったＩＤ情報がｎ回以上入力されると終了メッセージを出力して前記端末との接続を切離し、ＩＤ番号情報が正常でパスワード情報が異常のときは前記端末に入力エラーメッセージを出力し、さらに誤ったパスワード情報がｍ回以上入力されると前記ホストコンピュータの端末に警報メッセージを出力すると同時に、ダミー情報を端末へ送出することを特徴とするネットワークシステムの悪用防止方法。

【請求項３】　ホストコンピュータを中心に通信回線、ＬＡＮ等で接続された複数の端末を有し、且つ端末から送られるＩＤ番号情報及びパスワード情報が利用者登録と一致すると前記ホストコンピュータより端末に情報の出力を可能にしたネットワークシステムにおいて、前記端末から送られるＩＤ番号情報及びパスワード情報を利用者登録メモリに記憶された登録データをもとに判定し、ＩＤ番号情報が異常のとき、またはＩＤ番号情報が正常でパスワード情報が異常のとき前記端末に入力エラーメッセージを出力し、また誤ったＩＤ情報がｎ回以上入力されると終了メッセージを出力して端末との接続を切離し、またＩＤ番号情報が正常で誤ったパスワード情報がｍ回以上入力されると前記ホストコンピュータの端末に警報メッセージを出力する機能を有する判定処理手段と、この判定処理手段で誤ったパスワード情報がｍ回以上入力されたと判定されると起動され、ダミー情報メモリよりダミー情報を取込んでダミー用処理を実行し、前記端末へダミー情報を送出するダミー情報処理手段とを備えたことを特徴とするネットワークシステムの悪用防止装置。

2

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、ホストコンピュータを中心に通信回線、ＬＡＮ等で接続されたネットワークシステムの悪用防止方法及び装置に関する。

【０００２】

【従来の技術】ホストコンピュータを中心に通信回線、ＬＡＮ等で接続されたネットワークシステムとしては、例えば図４に示すような構成となっている。即ち、図４に示すようにホストコンピュータ管理室１にホストコンピュータ１１およびホストコンピュータ用端末とＣＲＴ１２が設置され、ホストコンピュータ管理者１３によって管理、運営、保守等が行われている。

【０００３】このホストコンピュータ１１は、通信回線３により端末群２と接続され、利用者２３は端末２１から自由にホストコンピュータ１１に対してアクセスすることにより、ホストコンピュータ１１の情報格納ＨＤ１４からホストコンピュータ情報が利用できるようになっている。

【０００４】ところで、このようなネットワークシステムを利用する場合、利用者２３はホストコンピュータ管理者１３にその旨を申請して利用者登録を行うことにより、利用者２３にはＩＤ番号（利用者登録番号）と利用者しか知らされないパスワード２４が与えられる。

【０００５】従って、利用者２３がネットワークシステムを利用する場合、端末２１にＩＤ番号とパスワード２４を入力し、利用者登録と一致すればホストコンピュータ１３と接続され、利用可能な状態となる。

【０００６】このネットワークシステムを利用するための条件としては、ＩＤ番号とパスワード２４とが利用者登録と一致するか否かをチェックするだけなので、万が一パスワード２４が第三者に知られた場合には利用可能になる。

【０００７】従来、このようなネットワークシステムの悪用防止方法としては、ホストコンピュータ１１と端末２１との接続時にＣＲＴ２２に図５に示すようなメッセージを表示させ、利用者２３がそのメッセージ内容をチェックすることにより第三者が悪用したか否かを判別していた。

【０００８】ここで、図５において、ＣＲＴ２２に表示されるメッセージ内容としては、前回の使用時間２２２、現在までの使用総時間２２３、現在までの使用回数２２４である。従って、このようなメッセージ内容では利用結果しか分からず、第三者に悪用された後で始めて利用者が気付くことになる。

【０００９】

【発明が解決しようとする課題】このように従来の悪用防止方法では、端末のＣＲＴに表示されるネットワーク

システムの利用状況を確認することで第三者に悪用されたどうかを判別しているため、特に第三者に知られては困る機密情報の場合には大きな問題である。

【００１０】本発明は、ネットワークシステムにおける悪用を未然に防止すると共に、利用者の情報を保護するネットワークシステムの悪用防止方法及び装置を提供することを目的とする。

【００１１】

【課題を解決するための手段】本発明は上記の目的を達成するため、ホストコンピュータを中心に通信回線、ＬＡＮ等で接続された複数の端末を有し、且つ端末から送られるＩＤ番号情報及びパスワード情報が利用者登録と一致すると前記ホストコンピュータより端末に情報の出力を可能にしたネットワークシステムにおいて、前記端末から送られるＩＤ番号情報及びパスワード情報を利用者登録メモリに記憶された登録データをもとに判定し、ＩＤ番号情報が異常のとき及びＩＤ番号情報が正常でパスワード情報が異常のとき前記端末に入力エラーメッセージを出力し、また誤ったＩＤ情報がｎ回以上入力されると終了メッセージを出力して端末との接続を切離し、またＩＤ番号情報が正常で誤ったパスワード情報がｍ回以上入力されると前記ホストコンピュータの端末に警報メッセージを出力する機能を有する判定処理手段と、この判定処理手段で誤ったパスワード情報がｍ回以上入力されたと判定されると起動され、ダミー情報メモリよりダミー情報を取込んでダミー用処理を実行し、前記端末にダミー情報を送出するダミー情報処理手段とを備えたものである。

【００１２】

【作用】このような構成のネットワークシステムの悪用防止装置にあっては、誤ったＩＤ情報がｎ回以上入力されると終了メッセージを出力して端末との接続が切離されるので、第三者にホストコンピュータより情報が出力されることがなく、またＩＤ番号情報が正常で誤ったパスワード情報がｍ回以上入力されるとホストコンピュータの端末に警報メッセージが出力されると同時に端末にダミー情報が送出されるので、ホストコンピュータ管理者によりＩＤ番号の使用停止手続をとることにより情報を保護できると共に、ダミー情報が出力されている間に再発防止のために端末使用者の追跡調査を行うことが可能となる。

【００１３】

【実施例】以下本発明の一実施例を図面を参照して説明する。ネットワークシステムの構成については図４と同様なので、ここではその説明を省略し、ホストコンピュータ内の第三者による悪用防止のための処理機能を図１に示すブロック図により説明する。

【００１４】図１において、３１は端末２１から送られてくるＩＤ番号情報及びパスワード情報を利用者登録メモリ３２に記憶されている登録データをもとに該当するか否かを判定する判定処理部で、この判定処理部３１はＩＤ番号情報が異常であったり、誤ったＩＤ情報がｎ回以上入力されると端末２１に入力エラーメッセージを出力したり、終了メッセージを出力する機能と、ＩＤ番号情報が正常であってもパスワード情報が異常であると端末に入力エラーメッセージを出力し、さらに誤ったパスワード情報がｍ回以上入力されるとホストコンピュータの端末１２に警報メッセージを出力する機能を有している。

【００１５】また、３３は判定処理部３１でＩＤ番号情報及びパスワード情報が共に正常であると判定されると、情報メモリ３４から情報を取込んで通常の処理を実行して端末２１へ送出するデータ処理部である。

【００１６】さらに、３５は判定処理部３１で誤ったパスワード情報がｍ回以上入力されたと判定されると起動され、ダミー情報メモリ３６よりダミー情報を取込んでダミー用処理を実行し、端末２１へダミー情報を送出するダミー情報処理部である。

【００１７】次に上記のように構成されたネットワークシステムの悪用防止処理機能の作用について図２及び図３に示すフローチャートを参照しながら説明する。いま、ホストコンピュータ１１は、端末２１からのアクセスを常時待っており（ステップＳ１）、アクセスがあると端末を接続し（ステップＳ２）、端末からの入力を受付ける状態となる。

【００１８】このような状態にあるとき、端末側からＩＤ番号情報が判定処理部３１に入力されると、この判定処理部１では利用者登録メモリ３２に該当する登録データがあるかどうかをチェックし（ステップＳ３）、登録データがなければ異常であるとして入力エラーメッセージを端末に発行する（ステップＳ４）。

【００１９】ここで、端末側から送られてくる誤ったＩＤ番号情報がｎ回以上入力されると（ステップＳ５）、端末に終了メッセージを発行して（ステップＳ６）、端末との接続を切離し（ステップＳ７）、初期状態に戻る。

【００２０】一方、上記ステップＳ３でＩＤ番号情報が正常であると判定されると、次に端末側から送られてくるパスワード情報が正常であるかどうかをチェックし（ステップＳ８）、異常であると入力エラーメッセージを端末に発行する（ステップＳ９）。

【００２１】ここで、端末側から送られてくる誤ったパスワード情報がｍ回以上入力されると（ステップＳ１０）、ホストコンピュータの端末に警報メッセージを表示し、ホストコンピュータ管理者に異常を知らせる（ステップＳ１１）と同時に、情報保護のためにＩＤ番号の使用停止手続を行う（ステップＳ１２）。

【００２２】また、再発防止の観点から、悪用かどうかを追跡するためにダミー用処理を実行し（ステップＳ１３）、ダミー情報を端末へ出力する。したがって、使用

5

者はあたかもホストコンピュータから情報が得られているものと思い込み、その間にホストコンピュータ管理者により端末使用者の追跡調査を行うことができる。

【００２３】一方、上記ステップＳ８でパスワード情報が正常であると判定されると、被害届けが出ているパスワードかどうかをチェックし（ステップＳ１４）、被害届けが出ているパスワードであれば、ステップＳ１１へ進み、入力ミスがm回以上あった後の処理と同様の処理が行われる。また、ステップＳ１４にて被害届けが出ていないパスワードであると判定した場合には、図５に示すような使用履歴を端末へ発行し（ステップＳ１５）、通常処理に移行する（ステップＳ１６）。

【００２４】このように本実施例では、端末から送られてくるＩＤ番号情報及びパスワード情報を判定処理部１により利用者登録メモリに記憶されている登録データをもとにチェックし、ＩＤ番号情報が異常のとき端末２１に入力エラーメッセージを出力し、さらに誤ったＩＤ情報がｎ回以上入力されると終了メッセージを出力し、またＩＤ番号情報が正常であってもパスワード情報が異常であると端末に入力エラーメッセージを出力し、さらに誤ったパスワード情報がm回以上入力されるとホストコンピュータの端末１２に警報メッセージを出力すると同時にダミー情報処理部３５よりダミー情報を端末２１へを送出するようにしたので、第三者によるネットワークシステムの悪用を未然に防止でき、また第三者が利用者のパスワードが解読された場合でも、その第三者の追跡を行って再発防止を図り、利用者の情報を保護することができる。

6

【００２５】

【発明の効果】以上述べたように本発明によれば、第三者によるネットワークシステムの悪用を未然に防止でき、また第三者が利用者のパスワードが解読された場合でも、その第三者の追跡を行って再発防止を図り、利用者の情報を保護することができるネットワークシステムの悪用防止方法及び装置を提供できる。

【図面の簡単な説明】

【図１】本発明によるネットワークシステムの悪用防止方法及び装置を説明するためのブロック図。

【図２】同実施例の作用を説明するためのフローチャートを示す図。

【図３】同じく図２に続くフローチャートを示す図。

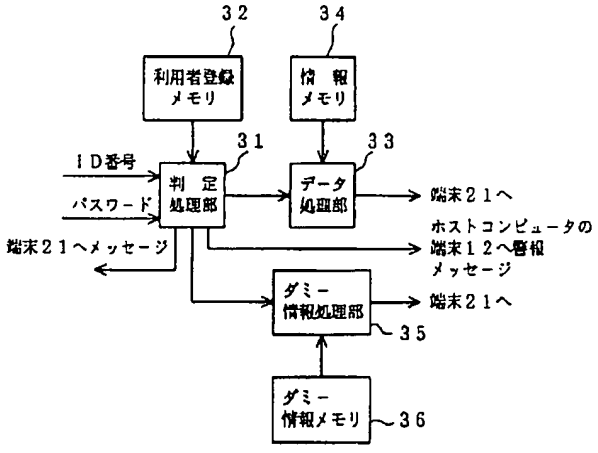
【図４】ネットワークシステムを説明するための構成例を示す図。

【図５】同システムにおいて、端末のＣＲＴに表示されたメッセージの説明図。

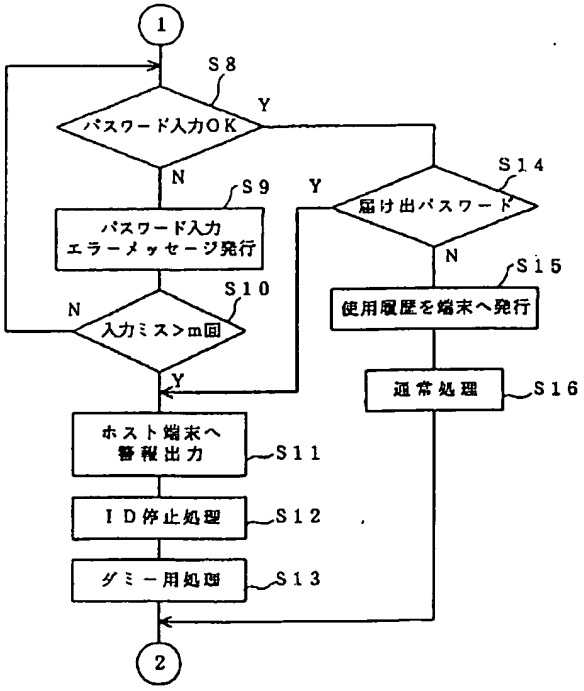
【符号の説明】

１１……ホストコンピュータ、１２……ホストコンピュータの端末、２１……端末、２２……ＣＲＴ、２４……パスワード、３１……判定処理部、３２……利用者登録メモリ、３３……データ処理部、３４……情報メモリ、３５……ダミー情報メモリ、３６……ダミー情報メモリ。

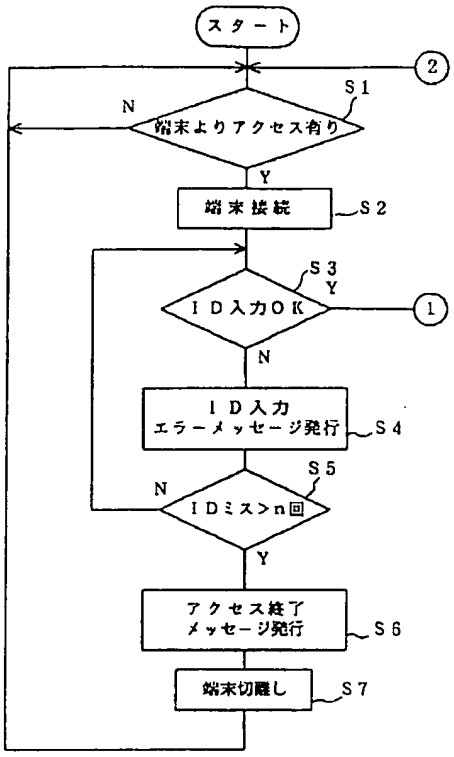
【図１】



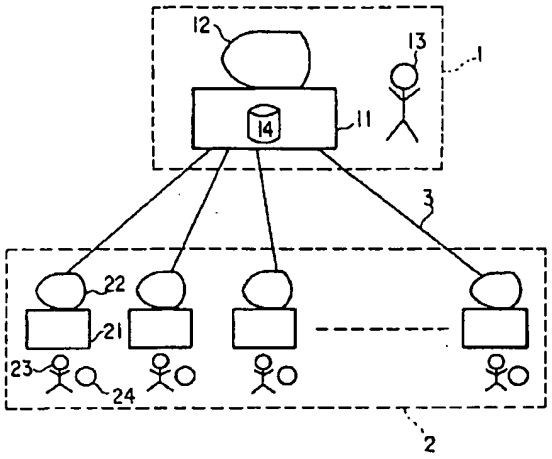
【図３】



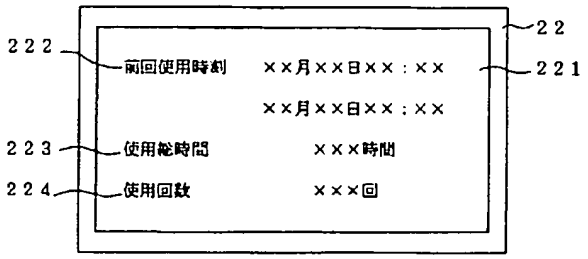
【図2】


スタート
2
S1
N
端末よりアクセス有り
Y
端末接続
S2
S3
Y
ＩＤ入力ＯＫ
1
N
ＩＤ入力
エラーメッセージ発行
S4
S5
N
ＩＤミス＞n回
Y
アクセス終了
メッセージ発行
S6
端末切離し
S7

【図4】


12
13
1
14
11
3
22
21
23
24
2

【図5】


222
前回使用時刻
××月××日××：××
××月××日××：××
22
221
223
使用総時間
×××時間
224
使用回数
×××回